I/S: A JOURNAL OF LAW AND POLICY FOR THE INFORMATION SOCIETY

Domesticating Programmatic Surveillance: Some Thoughts on the NSA Controversy

NATHAN ALEXANDER SALES*

On June 14, 2003, a Jordanian man named Ra'ed al-Banna landed at Chicago's O'Hare International Airport after a long flight from Amsterdam.[1] His paperwork was in perfect order: He held a legitimate Jordanian passport, he had obtained a visa authorizing him to work in the United States, and he had previously visited this country without incident. Nevertheless, al-Banna was pulled aside for a little extra scrutiny at the customs checkpoint. He'd been flagged by an automated system that national security officials use to analyze the huge troves of passenger reservation data that airlines must turn over when flying to the United States.[2] The officers who questioned him found him evasive, so they refused him entry and put him on the next flight home.

A year and a half later, a massive car bomb detonated in Hilla, Iraq, killing 132 police recruits. At the time, it was the deadliest suicide bombing Iraq had seen. "The driver was Ra'ed al-Banna. We know that because when authorities found the steering wheel of his car, his forearm was still chained to it."[3] It's impossible to know whether al-Banna would have carried out a similar attack in the

---

* Associate Professor of Law, Syracuse University College of Law. This Essay is based on testimony presented at a July 9, 2013 hearing of the Privacy and Civil Liberties Oversight Board.

[1] *See* Stewart A. Baker & Nathan Alexander Sales, *Homeland Security, Information Policy, and the Transatlantic Alliance*, *in* LEGAL ISSUES IN THE STRUGGLE AGAINST TERROR 277, 277-78 (John Norton Moore & Robert F. Turner eds., Carolina Academic Press 2010).

[2] 49 U.S.C. §§ 44909(c)(2), (3) (2012).

[3] Baker & Sales, *supra* note 1, at 278.

United States if he hadn't been turned away at the border. But we're fortunate not to have found out.

The recently disclosed NSA surveillance programs involve a different agency and different information. But they aim at the same objective—harnessing the power of big data to detect nascent threats before they can do harm—and raise the same vital questions about how to balance the competing demands of national security on the one hand and privacy and civil liberties on the other. This essay uses the NSA programs as a vehicle for thinking more broadly about bulk data collection. It begins by addressing the potential benefits of the practice. It then proposes some guiding principles to help ensure that any such surveillance is consistent with basic privacy and civil liberties values. It concludes with some observations on how well the NSA initiatives comport with these first principles, where they fall short, and how to modify them. The constitutional and statutory issues raised by the programs have been ably addressed elsewhere,[4] including by other participants in this symposium;[5] my contribution will focus more on the policy considerations than the legal ones.

I.

Based on press accounts, the NSA appears to be using the Foreign Intelligence Surveillance Act (FISA) to engage in *programmatic*, or *bulk*, surveillance—the collection of large amounts of data in an attempt to identify yet-unknown terrorists, spies, and other national security threats.[6]

---

[4] *See, e.g.*, Stephen G. Bradbury, *Understanding the NSA Programs: Bulk Acquisition of Telephone Metadata Under Section 215 and Foreign-Targeted Collection Under Section 702*, LAWFARE BLOG (August 30, 2013), http://www.lawfareblog.com/2013/08/steven-g-bradbury-on-understanding-the-nsa-progams-lawfare-research-paper-series/; *Oversight of the Administration's Use of FISA Authorities, Hearing Before the H. Comm. on the Judiciary*, 113d Cong. 84-103 (2013) (statement of Jameel Jaffer); David S. Kris, *On the Bulk Collection of Tangible Things*, LAWFARE RESEARCH PAPER SERIES (2013), *available at* http://www.lawfareblog.com/wp-content/uploads/2013/09/Lawfare-Research-Paper-Series-No.-4-2.pdf; Peter Margulies, *Evolving Relevance: The Metadata Program and the Delicate Balance of Secrecy, Deliberation, and National Security*, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2400809; NSA Programs, Hearing Before the H. Permanent Select Comm. on Intelligence, 113d Cong. __ (2013) (statement of Stephen I. Vladeck).

[5] *See, e.g.*, Laura Donohue, *FISA Reform*, 10 ISJLP 599 (2014); Katherine Strandberg, *Membership Lists, Metadata, and Freedom of Association's Specificity Requirement*, 10 ISJLP 327 (2014); John Yoo, *The Legality of the National Security Agency's Bulk Data Surveillance Programs*, 10 ISJLP 301 (2014).

[6] *See, e.g.*, William C. Banks, *Programmatic Surveillance and FISA: Of Needles in Haystacks*, 88 TEX. L. REV. 1633, 1635 (2010).

The first initiative—the so-called *telephony metadata* or *section 215* program—involves the use of court orders under FISA's business records authority (which was enacted by section 215 of the USA PATRIOT Act)[7] to collect transactional information about every telephone call placed over the networks of domestic telecommunications carriers—i.e., numbers dialed and call duration, but not content or location data.[8] At the risk of understatement, that is a monumental volume of data.[9] Once collected, these records are warehoused in special government databases and made available to intelligence analysts under fairly narrow circumstances. The FISA court's orders allow analysts to query the databases only if there is "reasonable suspicion, based on specific articulable facts, that a particular telephone number is associated with specified foreign terrorist organizations."[10] Originally, the NSA was responsible for determining whether the requisite suspicion was present in a given case, but President Obama has since directed the NSA to seek FISA court approval before querying the database, and the court has agreed to review such requests.[11] In 2012, analysts checked about 300 numbers against the database.[12] As this article goes to press, Congress is on the verge of enacting legislation that would substantially alter the program. Among other changes, the bill would bar the NSA from itself

---

[7] 50 U.S.C. § 1861 (2012).

[8] Glenn Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers Daily*, THE GUARDIAN (June 5, 2013), http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order.

[9] Recent indications are that the government is now collecting less than 30 percent of all domestic call metadata, down from nearly 100 percent in 2006, in part because of an ongoing shift from landlines to cell phones. Ellen Nakashima, *NSA Is Collecting less than 30 Percent of U.S. Call Data, Officials Say*, WASH. POST (Feb. 7, 2014), http://www.washingtonpost.com/world/national-security/nsa-is-collecting-less-than-30-percent-of-us-call-data-officials-say/2014/02/07/234a0e9e-8fad-11e3-b46a-5a3d0d2130da_story.html.

[10] Robert S. Litt, General Counsel, Office of the Director of National Intelligence, Panel Discussion: Newseum Special Program – NSA Surveillance Leaks: Facts and Fiction, 8 (June 26, 2013), *available at* http://www.dni.gov/index.php/newsroom/speeches-and-interviews/195-speeches-interviews-2013/887-transcript-newseum-special-program-nsa-surveillance-leaks-facts-and-fiction?tmpl=component&format=pdf.

[11] Brendan Sasso, *Secret Court Approves Obama's Changes to NSA Phone Sweeps*, NATIONAL JOURNAL (Feb. 6, 2014), http://www.nationaljournal.com/technology/secret-court-approves-obama-s-changes-to-nsa-phone-sweeps-20140206.

[12] *Id.*

collecting bulk telephony metadata. Instead, phone companies would hold the data, and NSA analysts could only acquire call records that are associated with a "specific selection term" (such as a particular phone number) and only with the prior approval of the FISA court.[13]

The FISA court repeatedly has upheld the section 215 program on both constitutional grounds (concluding that the acquisition of bulk telephony metadata was not a "search" within the meaning of the Fourth Amendment, largely on the strength of the third-party doctrine recognized in *Smith v. Maryland*[14] and other cases) and statutory ones (concluding that troves of data sought were tangible things that are relevant to an authorized investigation, as required by section 215).[15] By 2013, 15 different FISA court judges had approved the program in 35 separate rulings since its inception.[16] Other judges are more divided; in a pair of dueling rulings issued late last year, a federal judge in Washington, DC invalidated the program while another in Manhattan affirmed its legality.[17]

The second program—known as *PRISM* or *section 702*—uses court orders issued under section 702 of FISA[18] to collect the content of certain international communications. In particular, the NSA targets specific non-Americans who are reasonably believed to be located outside the country, and also engages in bulk collection of some foreign-to-foreign communications that happen to be passing through telecommunications infrastructure in the United States.[19] The FISA

---

[13] Charlie Savage, *Changes to Surveillance Bill Stoke Anger*, N.Y. TIMES (May 20, 2014), http://www.nytimes.com/2014/05/21/us/politics/changes-to-surveillance-bill-stoke-anger.html?_r=1 [hereinafter Savage, *Surveillance Bill*].

[14] 442 U.S. 735, 745-46 (1979).

[15] *See, e.g.*, *In Re* Application of the Federal Bureau of Investigation for an order requiring the production of tangible things from redacted, No. BR 13-109, slip op. at 3 (FISA Ct. 2013) *available at* http://www.uscourts.gov/uscourts/courts/fisc/br13-09-primary-order.pdf [hereinafter Section 215 Ruling]; *see also* Charlie Savage, *Extended Ruling by Secret Court Backs Collection of Phone Data*, N.Y. TIMES (Sept. 17, 2013), http://www.nytimes.com/2013/09/18/us/opinion-by-secret-court-calls-collection-of-phone-data-legal.html [hereinafter Savage, *Extended Ruling*].

[16] *Continued Oversight of U.S. Government Surveillance Authorities, Hearing Before the S. Comm. on the Judiciary*, 113d Cong. 8 (2013) (statement of James M. Cole, Deputy Attorney General, Department of Justice).

[17] *Compare* Klayman v. Obama, No. 13-0881, 2013 WL 6598728 (D.D.C. Dec. 16, 2013), *with* ACLU v. Clapper, No. 13 Civ. 3994, 2013 WL 6819708 (S.D.N.Y. Dec. 27, 2013).

[18] 50 U.S.C. § 1881a (2012).

[19] Barton Gellman & Laura Poitras, *U.S., British Intelligence Mining Data from Nine U.S. Internet Companies in Broad Secret Program*, WASH. POST (June 7, 2013),

court does not approve individual surveillance applications each time the NSA wishes to intercept these communications; instead, it issues once-a-year blanket authorizations.[20] As detailed below, in 2011 the FISA court struck down the program on constitutional and statutory grounds after the government disclosed that it was inadvertently intercepting a significant number of communications involving Americans;[21] the court later upheld the program when the NSA devised a technical solution that prevented such over-collection.[22]

Programmatic surveillance initiatives like these differ in simple yet fundamental ways from the traditional forms of monitoring with which many people are familiar—i.e., *individualized* or *particularized* surveillance. Individualized surveillance takes place when authorities have some reason to think that a specific, known person is breaking the law. Investigators will then obtain a court order authorizing them to collect information about the target, with the goal of assembling evidence that can be used to establish guilt in subsequent criminal proceedings. Individualized surveillance is common in the world of law enforcement, as under Title III of the Omnibus Crime Control and Safe Streets Act of 1968.[23] It is also used in national security investigations. FISA allows authorities to obtain a court order to engage in wiretapping if they demonstrate, among other things, probable cause to believe that the target is "a foreign power or an agent of a foreign power."[24]

By contrast, programmatic surveillance has very different objectives and is conducted in a very different manner. It usually involves the government collecting bulk data and then examining it to identify previously unknown terrorists, spies, and other national security threats. A good example of the practice is *link analysis*, in

---

http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_print.html; Jonathan Hall, *Washington Post Updates, Hedges On Initial PRISM Report*, FORBES (June 7, 2013), http://www.forbes.com/sites/jonathanhall/2013/06/07/washington-post-updates-hedges-on-initial-prism-report.

[20] 50 U.S.C. § 1881a(a) (2012).

[21] Redacted Case Name, Redacted Docket Number, slip op. at 80 (FISA Ct. 2011), *available at* http://www.lawfareblog.com/wp-content/uploads/2013/08/162016974-FISA-court-opinion-with-exemptions.pdf [hereinafter October 3, 2011 Section 702 Ruling].

[22] *See infra* note 94 and accompanying text.

[23] 18 U.S.C. § 2518 (2012).

[24] 50 U.S.C. § 1805(a)(2)(A) (2012).

which authorities compile large amounts of information, use it to map the social networks of known terrorists—has anyone else used the same credit card as Mohamed Atta?—and thus identify associates with whom they may be conspiring.[25] (It is also possible, at least in theory, to subject these large databases to *pattern analysis*, in which automated systems search for patterns of behavior that are thought to be indicative of terrorist activity, but it's not clear that the NSA is doing so here.) Suspects who have been so identified can then be subjected to further forms of monitoring to determine their intentions and capabilities, such as wiretaps under FISA or other authorities. In a sense, programmatic surveillance is the mirror image of individualized surveillance. With individualized monitoring, authorities begin by identifying a suspect and go on to collect information; with programmatic monitoring, authorities begin by collecting information and go on to identify a suspect.

Programmatic surveillance is a potentially powerful counterterrorism tool. The Ra'ed al-Banna incident is a useful illustration of how the technique, when coupled with old-fashioned police work, can identify possible threats who otherwise might escape detection. Another example comes from a 2002 Markle Foundation study, which found that authorities could have identified the ties among all 19 of the 9/11 hijackers if they had assembled a large database of airline reservation information and subjected it to link analysis.[26] In particular, two of the terrorists—Nawaf al-Hamzi and Khalid al-Mihdhar—were on a government watchlist after attending a January 2000 al-Qaeda summit in Malaysia. So they could have been flagged when they bought their tickets. Querying the database to see if any other passengers had used the pair's mailing addresses would have led investigators to three more hijackers, including Mohamed Atta, the plot's operational leader. Six others could have been found by searching for passengers who used the same frequent-flyer and telephone numbers as these suspects. And so on. Again, the Markle study concerns airline reservation data, not the communications data that are the NSA's focus. But it is still a useful illustration of the technique's potential.

The government claims that programmatic surveillance has been responsible for concrete and actual counterterrorism benefits, not just hypothetical ones. Officials report that PRISM has helped detect and

---

[25] MARK M. LOWENTHAL, INTELLIGENCE: FROM SECRETS TO POLICY 282 (5th ed. 2011).

[26] PROTECTING AMERICA'S FREEDOM IN THE INFORMATION AGE: A REPORT OF THE MARKLE FOUNDATION TASK FORCE 28 (2002), *available at* http://www.markle.org/sites/default/files/nstf_full.pdf; *see also* Baker & Sales, *supra* note 1, at 281-82.

disrupt about 50 terrorist plots worldwide, including ten in the United States.[27] Those numbers include Najibullah Zazi, who attempted to bomb New York City's subway system in 2009, and Khalid Ouazzani, who plotted to blow up the New York Stock Exchange.[28] Authorities further report that PRISM played an important role in tracking down David Headley, an American who aided the 2008 terrorist atrocities in Bombay, and later planned to attack the offices of a Danish newspaper that printed cartoons of Mohamed.[29] The government also claims at least one success from the telephony metadata program, though it has been coy about the specifics: "The NSA, using the business record FISA, tipped [the FBI] off that [an] individual had indirect contacts with a known terrorist overseas. . . . We were able to reopen this investigation, identify additional individuals through a legal process and were able to disrupt this terrorist activity."[30] Quite apart from foiling attacks, the government also argues that the NSA programs can conserve scarce investigative resources by helping officials quickly spot or rule out any foreign involvement in a domestic plot, as after the 2013 Boston Marathon bombing.[31]

These claims have to be taken with a few grains of salt. Some observers believe that the government could have discovered the plots using standard investigative techniques, and without resorting to extraordinary methods like programmatic surveillance.[32] The metadata program has elicited special skepticism: The President's Review Group on Intelligence and Communications Technologies bluntly concluded that "the information contributed to terrorist investigations by the use of section 215 telephony meta-data was not essential to preventing attacks and could readily have been obtained

---

[27] Sean Sullivan, *NSA Head: Surveillance Helped Thwart More Than 50 Terror Plots*, WASH. POST (June 18, 2013), http://www.washingtonpost.com/blogs/post-politics/wp/2013/06/18/nsa-head-surveillance-helped-thwart-more-than-50-terror-attempts/.

[28] *Id.*

[29] *Id.*

[30] *Id.*

[31] Ellen Nakashima, *NSA Chief Defends Collecting Americans' Data*, WASH. POST (Sept. 25, 2013), http://www.washingtonpost.com/world/national-security/nsa-chief-defends-collecting-americans-data/2013/09/25/5db2583c-25f1-11e3-b75d-5b7f66349852_story.html.

[32] Abby Ohlheiser, *The NSA's Best Defense of PRISM Didn't Even Last a Week*, ATLANTIC WIRE (June 11, 2013), http://www.thewire.com/national/2013/06/nsas-only-terrorist-defense-prism-didnt-even-last-week/66143/.

in a timely manner using conventional section 215 orders."[33] The Privacy and Civil Liberties Oversight Board reached the same conclusion.[34] (Judicial opinion is split on the program's value. One judge has expressed "serious doubts" about its utility,[35] while another has concluded that its effectiveness "cannot be seriously disputed.")[36] Furthermore, we should always be cautious when evaluating the merits of classified intelligence initiatives on the basis of selective and piecemeal revelations, as officials might tailor the information they release in a bid to shape public opinion.[37] But even if specific claimed successes remain contested, programmatic surveillance in general can still be a useful counterterrorism technique.

As these examples imply, effective programmatic surveillance often requires huge troves of information—e.g., large databases of airline reservations, compilations of metadata concerning telephonic and internet communications, and so on. This is why it typically will not be feasible to limit bulk collection to particular, known individuals who are already suspected of being terrorists or spies. Some officials have defended the NSA programs by pointing out that, "[i]f you're looking for the needle in a haystack, you have to have the haystack."[38] That metaphor doesn't strike me as terribly helpful; rummaging around in a pile of hay is, after all, a paradigmatic image of futility. But, the idea can be expressed in a more compelling way. Programmatic surveillance cannot be done in a particularized manner. The whole point of the technique is to identify unknown threats to the national security; by definition, it cannot be restricted to threats that have already been identified. We can't limit programmatic

---

[33] THE PRESIDENT'S REVIEW GROUP ON INTELLIGENCE AND COMMUNICATIONS TECHNOLOGIES, REPORT AND RECOMMENDATIONS: LIBERTY AND SECURITY IN A CHANGING WORLD 104 (2013) [*hereinafter* PRESIDENT'S REVIEW GROUP].

[34] PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, REPORT ON THE TELEPHONE RECORDS PROGRAM CONDUCTED UNDER SECTION 215 OF THE USA PATRIOT ACT AND ON THE OPERATIONS OF THE FOREIGN INTELLIGENCE SURVEILLANCE COURT 11 (2013), *available at* http://www.pclob.gov/All%20Documents/Report%20on%20the%20Telephone%20Records%20Program/PCLOB-Report-on-the-Telephone-Records-Program.pdf.

[35] Klayman v. Obama, No. 13-0881, 2013 WL 6598728, at *17 (D.D.C. Dec. 16, 2013).

[36] ACLU v. Clapper, No. 13 Civ. 3994, 2013 WL 6819708, at *25 (S.D.N.Y. Dec. 27, 2013).

[37] JAMES BAMFORD, BODY OF SECRETS: ANATOMY OF THE ULTRA-SECRET NATIONAL SECURITY AGENCY: FROM THE COLD WAR THROUGH THE DAWN OF A NEW CENTURY 384 (2001).

[38] Dana Bash & Tom Cohen, *Officials Cite Thwarted Plots, Oversight in Defending Surveillance*, CNN (June 19, 2013), http://www.cnn.com/2013/06/18/politics/nsa-leaks/index.html.

surveillance to the next Mohamed Atta when we have no idea who the next Mohamed Atta is—and when the goal of the exercise is indeed to identify the next Mohamed Atta.

Programmatic surveillance thus can help remedy some of the difficulties that arise when monitoring covert adversaries like international terrorists. FISA and other particularized surveillance tools are useful when authorities want to monitor targets whose identities are already known. But they are less useful when authorities are trying to identify unknown targets. The problem arises because, in order to obtain a wiretap order from the FISA court, the government usually must demonstrate probable cause to believe that the target is a foreign power or agent of a foreign power.[39] This is a fairly straightforward task when the target's identity is already known—e.g., a diplomat at the Soviet embassy in Washington, DC. But the task is considerably more difficult when the government's reason for surveillance is to detect targets who are presently unknown—e.g., al-Qaeda members who operate in the shadows. How can you convince the FISA court that Smith is an agent of a foreign power when you know nothing about Smith—his name, nationality, date of birth, location, or even whether he is a single person or several dozen? The government typically won't know those things unless it has collected some information about Smith—such as by surveilling him. And there's the rub. Programmatic monitoring helps avoid the crippling Catch-22 that can arise under particularized surveillance regimes like FISA: officials can't surveil unless they show that the target is a spy or terrorist, but sometimes they can't show that an unknown target is a spy or terrorist unless they have surveilled him.

II.

While programmatic surveillance can be an important counterterrorism tool, it also—given the sweeping scope of the data collection on which it usually relies—raises profound concerns about civil liberties and privacy. These concerns are not merely hypothetical. To take just a few justifiably notorious examples of abusive monitoring, albeit of the particularized rather than programmatic variety, the FBI repeatedly wiretapped Dr. Martin Luther King and his associates, purportedly to discover whether the civil rights icon had any ties to the Soviet Union.[40] And during the 1964 presidential

---

[39] 50 U.S.C. § 1805(a)(2)(A) (2012).

[40] David J. Garrow, *The FBI and Martin Luther King*, THE ATLANTIC (July 2002), http://www.theatlantic.com/past/issues/2002/07/garrow.htm.

campaign, LBJ aide Bill Moyers—yes, *that* Bill Moyers—directed the FBI to dig around for evidence that some of Barry Goldwater's staffers were homosexuals.[41] The possibility of abuse makes it critical to establish a set of first principles to govern when and how programmatic monitoring is to be conducted. It is especially important to think about these baseline rules now, when the technique is still in its relative youth. This will allow programmatic surveillance to be nudged in privacy-protective directions as it develops into maturity. The critical question is how to take advantage of its potentially significant national security benefits without running afoul of fundamental civil liberties and privacy values. In other words, what can be done to domesticate programmatic surveillance?

This is not the place to flesh out the precise details of the ideal surveillance regime, but we can identify certain basic principles that academics, policymakers, and others should consider when thinking about bulk data collection and analysis. Two broad categories of principles should govern any such system; one concerns its formation, the other its implementation. First, there are the *architectural* or *structural* considerations—the principles that address when programmatic surveillance should take place, the process by which such a regime should be adopted, and how the system should be organized. Second, there are the *operational* considerations—the principles that inform the manner in which programmatic surveillance should be carried out in practice.

A.

As for the structural considerations, one of the most important is what might be called an *anti-unilateralism* principle. A system of programmatic surveillance should not be put into effect on the say-so of the executive branch, but rather should be a collaborative effort that involves Congress (in the form of authorizing legislation) or the judiciary (in the form of FISA court review of the initiatives).[42] An example of the former is FISA itself, which Congress enacted in 1978. At the time, the NSA was engaged in bulk collection, without judicial approval, of certain international communications into and out of the United States—namely, by tapping into offshore telecommunications cables and by eavesdropping on satellite based radio signals. FISA's

---

[41] Laurence H. Silberman, *Hoover's Institution*, WALL ST. J. (JULY 20, 2005), http://online.wsj.com/news/articles/SB112182505647390371.

[42] *See generally* JACK GOLDSMITH, THE TERROR PRESIDENCY 123-26, 205-07 (2007).

famously convoluted definition of "electronic surveillance"[43] preserved these preexisting practices even as Congress was imposing a new requirement of judicial approval for other kinds of monitoring.[44] An example of the latter concerns the warrantless Terrorist Surveillance Program, under which the NSA was intercepting, outside the FISA framework, certain communications between suspected al-Qaeda figures overseas and people located in the United States. After that program's existence was revealed in late 2005, the executive branch persuaded the FISA court to issue orders allowing it to proceed subject to various limits.[45] (That accommodation eventually proved unworkable, and the executive then worked with Congress to put the program on a more solid legislative footing through the temporary Protect America Act of 2007[46] and the permanent FISA Amendments Act of 2008.)[47]

Anti-unilateralism is important for several reasons. To take the most obvious, Congress and the courts can help prevent executive overreach.[48] The risk of abuse is lessened if the executive branch must enlist its partners before commencing a new surveillance initiative. Congress might decline to permit bulk collection in circumstances where it concludes that ordinary, individualized monitoring would suffice, or it might authorize programmatic surveillance subject to various privacy protections. In addition, inviting many voices to the decision-making table increases the probability of sound outcomes. More participants with diverse perspectives can also help mitigate the groupthink tendencies to which the executive branch is sometimes

---

[43] 50 U.S.C. § 1801(f) (2012).

[44] David S. Kris, *Modernizing the Foreign Intelligence Surveillance Act*, *in* LEGISLATING THE WAR ON TERROR: AN AGENDA FOR REFORM 217, 224-25 (Benjamin Wittes ed., 2009).

[45] David Kris, *A Guide to the New FISA Bill, Part II*, BALKINIZATION (June 22, 2008), http://balkin.blogspot.com/2008/06/guide-to-new-fisa-bill-part-ii.html.

[46] Pub. L. No. 110-55, 121 Stat. 552 (2007).

[47] Pub. L. No. 110-261, 122 Stat. 2436 (2008).

[48] *See, e.g.*, JACK GOLDSMITH, POWER AND CONSTRAINT: THE ACCOUNTABLE PRESIDENCY AFTER 9/11, at xv (2012) ("[D]emocratic and judicial forces change presidential authorities and actions deemed imprudent or wrong and constrain presidential discretion in numerous ways."). *But see* ERIC A. POSNER & ADRIAN VERMEULE, THE EXECUTIVE UNBOUND: AFTER THE MADISONIAN REPUBLIC 4 (2010) (arguing that we now live in an "age after the separation of powers, and the legally constrained executive is now a historical curiosity").

subject.[49] If we're going to engage in programmatic surveillance, it should be the result of give and take among all three branches of the federal government, or at least between its two political branches, not the result of executive edict.

A second principle follows from the first: Programmatic surveillance should, wherever possible, have *explicit statutory authorization*. Congress does not "hide elephants in mouseholes,"[50] the saying goes, and we should not presume that Congress meant to conceal its approval of a potentially controversial programmatic surveillance system in the penumbrae and interstices of obscure federal statutes. Instead, Congress normally should use express and specific legislation when it wants to okay bulk data collection. Clear laws will help remove any doubt about the authorized scope of the approved surveillance, thereby promoting legal certainty. Express congressional backing also helps give the monitoring an air of legitimacy. And, a requirement that programmatic surveillance usually should be approved by clear legislation helps promote accountability by minimizing the risk of congressional shirking.[51] If the political winds shift, and a legislatively approved program becomes unpopular, Congress will not be able to hide behind an ambiguous statutory grant of power and deflect responsibility to the President.

Of course, exacting legislative clarity may not be possible in all cases. Sometimes, explicit statutory language might compromise intelligence sources and methods, enabling surveillance targets to evade detection[52] or provoking a diplomatic row.[53] But some degree of clarity often will be feasible, and the Protect America Act and FISA Amendments Act are good examples of what the process could look like. In both cases, Congress clearly and unambiguously approved

---

[49] *See, e.g.*, Steve Smith, *Groupthink and the Hostage Rescue Mission*, 15 BRIT. J. POL. SCI. 117 (1984).

[50] Whitman v. Am. Trucking Ass'ns, 531 U.S. 457, 468 (2001).

[51] *See, e.g.*, Nicholas Quinn Rosenkranz, *Federal Rules of Statutory Interpretation*, 115 HARV. L. REV. 2085, 2155 (2002) (emphasizing that "ambiguity allows Congress to evade accountability").

[52] *See, e.g.*, CIA v. Sims, 471 U.S. 159, 167 (1985).

[53] *See, e.g.*, Peter P. Swire, *The System of Foreign Intelligence Surveillance Law*, 72 GEO. WASH. L. REV. 1306, 1323 (2004).

monitoring that the executive branch previously claimed[54] was within the President's inherent constitutional powers and, in any event, was implicitly authorized by a combination of FISA (which at the time made it unlawful to engage in electronic surveillance "except as authorized by [statute]")[55], the 9/11 Authorization for Use of Military Force (which allows the president to use "all necessary and appropriate force" against those responsible for the attacks),[56] and the Supreme Court's decision in *Hamdi v. Rumsfeld* (which interpreted the AUMF's reference to "all necessary and appropriate force" to include "fundamental and accepted" incidents of war, such as detention and perhaps, by implication, electronic surveillance).[57]

Next, there is the question of *transparency*. Whenever possible, programmatic surveillance systems should be adopted through open and transparent debates that allow an informed public to meaningfully participate. The systems also should be operated in as transparent a manner as possible. This in turn requires the government to reveal enough information about the initiative, even if at a fairly high level of generality, that the public is able to effectively weigh its benefits and costs. It is especially important that officials provide fairly granular details about a given program's claimed benefits, such as its value in foiling terrorist plots, so the public can evaluate whether those gains are worth the resulting tradeoffs.

Transparency is important because it helps promote accountability; it enables the public to hold their representatives in Congress and the executive branch responsible for the choices they make. "[I]nformed public opinion is the most potent of all restraints upon misgovernment."[58] Transparency also fosters democratic participation, ensuring that the people are ultimately responsible for deciding our national security policies. And, it can help dispel suspicions about programs that initially might seem nefarious but end up looking innocuous when their details are known.[59] Again, perfect

---

[54] Letter from William E. Moschella, Assistant Att'y Gen., Off. of Legis. Aff., U.S. Dep't of Justice., to Pat Roberts, Chairman, Senate Select Comm. on Intelligence, et al. (Dec. 22, 2005), *available at* http://www.fas.org/irp/agency/doj/fisa/doj122205.pdf.

[55] 50 U.S.C. § 1809(a)(1) (2000).

[56] Pub. L. No. 107-40, § 2(a), 115 Stat. 224 (2001).

[57] 542 U.S. 507, 518 (2004).

[58] Grossjean v. Am. Press Co., 297 U.S. 233, 250 (1936).

[59] *See, e.g.*, Richard Gid Powers, *Introduction* to DANIEL PATRICK MOYNIHAN, SECRECY: THE AMERICAN EXPERIENCE 58 (1998) (emphasizing that a lack of transparency "gives rise to fantasies that corrode belief in the possibilities of democratic government").

transparency will not always be feasible—a public debate about the fine-grained details of national security surveillance can compromise extremely sensitive intelligence sources and methods. But transparency should be the default rule, and even where the government's operational needs rule out detailed disclosures, a generic description of a proposed program is better than none at all.

Finally, any programmatic surveillance regime should observe an *anti-mission-creep* principle. Bulk data collection should only be used to investigate and prevent terrorism, espionage, and other serious threats to the national security. It should be off limits in regular criminal investigations. Moreover, if programmatic surveillance happens to turn up evidence of ordinary crime, intelligence officials normally should not be able to refer it to their law enforcement counterparts for prosecution—though there should be an exception for truly grave crimes, such as offenses involving a risk of death or serious bodily injury and crimes involving the exploitation of children. This is a simple matter of costs and benefits. The upside of preventing deadly terrorist attacks and other national security perils can be so significant that we as a nation may be willing to sanction extraordinary investigative techniques like bulk data collection. But the calculus looks very different where the promised upside is prosecuting garden-variety crimes like income tax evasion or insurance fraud. We might be willing to tolerate an additional burden on our privacy interests to stop the next 9/11, but that doesn't mean we should make the same sacrifice to stop tax cheats and fraudsters.

B.

As for the operational considerations, among the most important is the need for *external checks* on programmatic surveillance. In particular, bulk data collection should have to undergo some form of judicial review, such as by the FISA court, in which the government demonstrates that it meets the applicable constitutional and statutory standards. Ideally, the judiciary would give its approval before collection begins. But this will not always be possible, in which case timely post-collection judicial review will have to suffice. (FISA has a comparable mechanism for temporary warrantless surveillance in emergency situations.)[60] Programmatic surveillance also should be subject to robust congressional oversight. This could take a variety of forms, including informal consultations with members of Congress when designing the surveillance regime (including, at a minimum, congressional leadership and members of the applicable committees),

[60] 50 U.S.C. § 1805(e) (2012).

as well as regular briefings to appropriate personnel on the operation of the system and periodic oversight hearings.

Of course, judicial review in the context of bulk collection won't necessarily look the same as it does in the familiar setting of individualized monitoring of specific targets. If investigators want to examine the telephony metadata associated with a particular terrorism suspect, they can apply to the FISA court for a pen register or trap and trace order upon a showing that the information sought is relevant to an ongoing national security investigation.[61] But, as explained above, that kind of particularized showing often won't be possible where authorities are dealing with unknown threats, and where the very purpose of the surveillance is to identify those threats. In these situations, reviewing courts may find it necessary to allow the government to collect large amounts of data without individualized suspicion. This doesn't mean that privacy safeguards must be abandoned and the executive given free rein. Instead, courts could be tasked with scrutinizing the initiative's overall structure and operation to determine its compatibility with constitutional and statutory requirements. And courts further could require authorities to demonstrate some level of individualized suspicion before accessing the data that has been collected. Protections for privacy and civil liberties thus can migrate from the collection phase of the intelligence cycle to earlier and later stages, such as the systems design and analysis stages.[62]

In more general terms, because programmatic surveillance involves the collection of large troves of data, it likely means some dilution of the familiar ex ante restrictions that protect privacy by constraining the government from acquiring information in the first place. It therefore becomes critically important to devise meaningful ex post safeguards that can achieve similar forms of privacy protection. In short, restrictions on the government's ability to access and use data that it has gathered must substitute for restrictions on the government's ability to gather that data at all; what I have elsewhere called *use limits* must stand in for *collection limits*.[63]

This sort of oversight by the courts and Congress provides an obvious, first-order level of protection for privacy and civil liberties—an external veto serves as a direct check on possible executive

---

[61] 50 U.S.C. § 1842 (2012).

[62] *See* LOWENTHAL, *supra* note 25, at 57-70 (describing various stages of the intelligence cycle, including collection, processing and exploitation, analysis, and dissemination).

[63] Nathan Alexander Sales, *Run for the Border: Laptop Searches and the Fourth Amendment*, 43 U. RICH. L. REV. 1091, 1124-27 (2009).

misconduct. Judicial and legislative checks also offer an important second-order form of protection. The mere possibility of an outsider's veto can have a chilling effect on executive misconduct, discouraging officials from questionable activities that would have to undergo, and might not survive, external review.[64] Moreover, external checks can channel the executive's scarce resources into truly important surveillance and away from relatively unimportant monitoring. This is so because oversight increases the administrative costs of collecting bulk data—e.g., preparing a surveillance application, persuading the judiciary to approve it, briefing the courts and Congress about how the program has been implemented, and so on. These increased costs encourage the executive to prioritize collection that is expected to yield truly valuable intelligence and, conversely, to forego collection that is expected to produce information of lesser value.

In addition to oversight by outsiders, a programmatic surveillance regime also should feature a system of *internal checks* within the executive branch, to review collection before it occurs, after the fact, or both. As for the ex ante checks, internal watchdogs should be charged with scrutinizing proposed bulk collection to verify that it complies with the applicable constitutional and statutory rules, and also to ensure that appropriate protections are in place for privacy and civil liberties. The Justice Department's Office of Intelligence is a well known example. The unit, which presents the government's surveillance applications to the FISA court, subjects these requests to exacting scrutiny with the goal of increasing the likelihood of surviving judicial review.[65] Indeed, the office has a strong incentive to ensure that the applications it presents are airtight, so as to preserve its credibility with the FISA court.[66] Ex post checks include such commonplace mechanisms as agency-level inspectors general, who can audit bulk collection programs, assess their legality, and make policy recommendations to improve their operation, as well as entities like the Privacy and Civil Liberties Oversight Board, which perform similar functions across the executive branch as a whole. Another important ex post check is to offer meaningful whistleblower protections to officials who know about programs that violate constitutional or statutory requirements. Allowing officials to bring their concerns to ombudsmen within the executive branch (and then eventually to Congress) can help root out lawlessness and also relieve

---

[64] *See, e.g.*, Nathan Alexander Sales, *Self-Restraint and National Security*, 6 J. NAT'L SEC. L. & POL'Y 227, 280 (2012).

[65] *Id.* at 259-60.

[66] *Id.* at 285-86.

the felt necessity of leaking information about highly classified programs to the media.

These and other internal checks can achieve all three of the benefits promised by traditional judicial and legislative oversight—executive branch watchdogs can veto surveillance they conclude would be unlawful, the mere possibility of such vetoes can chill overreach, and increasing the costs of monitoring can redirect scarce resources toward truly important surveillance. External and internal checks thus operate together as a system; the two types of restraints are rough substitutes for one another. If outside players like Congress and the courts are subjecting the executive's programmatic surveillance activities to especially rigorous scrutiny, the need for comparably robust safeguards within the executive branch tends to diminish. Conversely, if the executive's discretion is constrained internally through strict approval processes, audit requirements, and so on, the legislature and judiciary may choose not to hold the executive to the exacting standards they otherwise would. In short, certain situations may have less need to use traditional interbranch separation of powers and checks and balances to protect privacy and civil liberties because the executive branch is subject to an "internal separation of powers"[67] that can accomplish much the same thing.

A word of caution: It is important not to take in-house review too far. Internal oversight can do more than deter overreach. It can also deter necessary national security operations, with potentially deadly results. The pre-9/11 information sharing wall is a notorious example of an internal check gone awry. The predecessor of DOJ's Office of Intelligence interpreted FISA to sharply restrict intelligence officials from sharing information or otherwise coordinating with their law enforcement counterparts, leading one prophetic FBI agent to lament on the eve of 9/11 that "someday somebody will die."[68] DOJ lawyers were so committed to the wall that one senior official successfully lobbied the chief judge of the FISA court to issue an order formally adopting the wall requirements, which up to then had only taken the form of internal Justice Department guidelines.[69] There are other examples as well. In the 1990s, executive branch lawyers vetoed CIA

---

[67] Neal Kumar Katyal, *Internal Separation of Powers: Checking Today's Most Dangerous Branch from Within*, 115 YALE L.J. 2314, 2317 (2006).

[68] NATIONAL COMMISSION ON TERRORIST ATTACKS UPON THE UNITED STATES, THE 9/11 COMMISSION REPORT 271 (2004).

[69] STEWART A. BAKER, SKATING ON STILTS: WHY WE AREN'T STOPPING TOMORROW'S TERRORISM TODAY 57 (2010), *available at* http://www.skatingonstilts.com/skating-on-stilts/tired-of-reading-chapters-backwards.html.

plans to use targeted killing against Osama bin Laden, and members of the armed forces' Judge Advocate General corps have occasionally objected to strikes on particular targets even though they would be permissible under the laws of war.[70] There is no universally applicable answer to the question, *how much internal oversight is enough?* The right balance cannot be known a priori, but rather must be struck on a case by case basis taking account of the highly contingent and unique circumstances presented by a given surveillance program, the threat it seeks to combat, the privacy concerns it raises, and other factors.

A third operational consideration is the need for strong *minimization requirements*. Virtually all surveillance raises the risk that officials will intercept innocuous data in the course of gathering evidence of illicit activity. Inevitably, some chaff will be swept up with the wheat. The risk is especially acute with programmatic surveillance, in which the government assembles large amounts of data in the search for clues about a small handful of terrorists, spies, and other national security threats.[71] Minimization is one way to deal with the problem. Minimization rules limit what the government may do with data that does not appear pertinent to a national security investigation—e.g., how long it may be retained, the conditions under which it will be stored, the rules for accessing it, the purposes for which it may be used, the entities with which it may be shared, and so on. Congress appropriately has required intelligence officials to adopt minimization procedures, both under FISA's longstanding particularized surveillance regime[72] and under the more recent authorities permitting bulk collection.[73] But the rules need not be identical. Because programmatic surveillance often involves the acquisition of a much larger trove of non-pertinent information, the minimization rules for bulk collection ideally would contain stricter limits on the use of inadvertently collected information for purposes unrelated to national security. In other words, the minimization procedures should reflect the *anti-mission-creep* principle described above.

Finally, programmatic surveillance systems should have *technological safeguards* that protect privacy and civil liberties by restricting access to sensitive information and tracking what officials

---

[70] Sales, *Self-Restraint*, *supra* note 63, at 247-56.

[71] LOWENTHAL, *supra* note 25, at 72-73.

[72] 50 U.S.C. §§ 1801(h), 1805(a)(3) (2012).

[73] 50 U.S.C. §§ 1881a(c)(1)(A), (e).

do with it.[74] As Larry Lessig has emphasized, software features that make it impossible to engage in certain undesirable conduct can substitute for legal prohibitions on the same behavior; "code is law."[75] In particular, permissioning and authentication technologies can help ensure that sensitive databases are only available to officials who need them to perform various counterterrorism functions. And auditing tools can track who accesses the information, when, in what manner, and for what purposes. These mechanisms show promise but thus far have a mixed record at preventing unauthorized access to and use of sensitive data. Access logs helped the State Department quickly identify and discipline the outside contractors who improperly accessed the private passport files of various presidential candidates in 2008.[76] But government employees like Edward Snowden and Bradley Manning obviously have been able to exfiltrate huge amounts of classified information from protected systems, either because technological controls were not in place or because they were able to evade them. Even if these mechanisms are not now an infallible safeguard against abuse, the basic principle seems sound: A commitment to privacy can be baked into a programmatic surveillance regime at the level of systems architecture.

III.

Judged by these standards, how well do the NSA initiatives measure up? As far as we can tell from the incomplete publicly available information, they fare well along several dimensions. But in other respects the programs should be adjusted to better conform to the first principles sketched out above. Several relatively modest reforms would preserve the essential features of the programs but ensure more robust protections for privacy and civil liberties.

Before turning to areas that need improvement, it's worth spending a few moments considering what the government has gotten right. One of the most noteworthy features of the NSA programs is their rejection of unilateralism. Rather than justifying the collection of international communications and telephony metadata on the basis of

---

[74] *See, e.g.*, BAKER, *supra* note 68, at 334-41; MARKLE FOUNDATION, *supra* note 25, at 15, 17, 19, 33.

[75] LAWRENCE LESSIG, CODE: VERSION 2.0, at 5-6 (2006), *available at* http://codev2.cc/download+remix/Lessig-Codev2.pdf.

[76] Glenn Kessler, *Rice Apologizes For Breach of Passport Data*, WASH. POST. (Mar. 22, 2008), http://www.washingtonpost.com/wp-dyn/content/article/2008/03/21/AR2008032100377.html.

its own constitutional authorities, the executive branch in both instances has sought to ground its conduct in statutory powers conferred on it by Congress. This anti-unilateralism is especially significant because it is something of an historical anomaly; the executive routinely has undertaken national security surveillance without legislative backing. Consider, for example, wiretaps in the pre-FISA era, which were grounded solely in the president's constitutional powers,[77] or the executive's unilateral conduct of physical searches before FISA was amended in the 1990s to expressly authorize that activity,[78] or the warrantless Terrorist Surveillance Program of the early 2000s.

Of course, Congress has been much more explicit about approving the section 702 program than the telephony metadata initiative. The latter is said to be based on section 215 of the USA PATRIOT Act, which allows officials to obtain a FISA court order requiring the production of "any tangible things" upon a showing that they are "relevant" to an authorized national security investigation.[79] Section 215 is often understood as FISA's counterpart to the rules governing grand jury subpoenas. Yet the government is using it to collect a great deal more information than a typical subpoena obtains, and at least one legislator who was actively involved in crafting the statute claims that Congress never intended it to be used in this way.[80] To put it mildly, section 215 is a more roundabout authorization than section 702.

Yet Congress has been involved in approving the metadata program, albeit in a way that is less specific and transparent than ideal. Section 215 is a temporary provision that is subject to periodic legislative renewals. During the congressional debates over reauthorization in 2010 and 2011, the intelligence community prepared classified briefing materials that laid out unusually vivid details about the program.[81] The briefing papers described what

---

[77] *See* Swire, *supra* note 53, at 1313-14.

[78] *See* William C. Banks & M.E. Bowman, *Executive Authority for National Security Surveillance*, 50 AM. U. L. REV. 1, 77 (2000).

[79] 50 U.S.C. §§ 1861(a)(1), (b)(2)(A) (2012).

[80] *See* Letter from Rep. F. James Sensenbrenner, Jr. to Attorney General Eric H. Holder, Jr. (June 6, 2013), *available at* http://sensenbrenner.house.gov/uploadedfiles/sensenbrenner_letter_to_attorney_general_eric_holder.pdf.

[81] *See* Office of Legislative Affairs, Dep't of Justice, Report on the National Security Agency's Bulk Collection Programs Affected by USA PATRIOT Act Reauthorization (2009), *available at*

information is collected, when the database may be queried, and—critically—the fact that the program is operated "pursuant to the 'business records' provision of the Foreign Intelligence Surveillance Act (FISA) (commonly referred to as 'section 215')," [82] as well as the fact that the FISA court had approved the government's interpretation. Officials further asked that the materials be shared with "all Members of Congress." [83] In 2010 and again the following year, the Chairman and Vice Chairman of the Senate Select Committee on Intelligence circulated "Dear Colleague" letters encouraging senators to review the briefing. [84] On the House side, in 2010 a member of the Permanent Select Committee on Intelligence made a floor statement urging colleagues to review the materials. [85] (He does not appear to have renewed the invitation in 2011.) In addition to making these written materials available, administration officials reportedly conducted 13 in-person classified briefings for members about the section 215 program. [86]

Members of Congress who learned from these briefings that the executive branch was interpreting section 215 to authorize the telephony metadata program, and who then voted to reauthorize that legislation, can be said at some level to have embraced the executive's interpretation. Congress in 2001 may not have understood section 215 as anything more than a routine subpoena-like tool for the national security context. But Congress in 2010 and 2011 was put on notice that the executive branch was now reading the statute more expansively to authorize bulk data collection. In any event, the critical point is not, as some judges and commentators have concluded, that

---

http://www.dni.gov/files/documents/2009_CoverLetter_Report_Collection.pdf [*hereinafter* 2009 DOJ Report]; Office of Legislative Affairs, Dep't of Justice, Report on the National Security Agency's Bulk Collection Programs Affected by USA PATRIOT Act Reauthorization (2011), *available at* http://www.dni.gov/files/documents/2011_CoverLetters_Report_Collection.pdf [*hereinafter* 2011 DOJ Report].

[82] 2009 DOJ REPORT, *supra* note 80, at 2; 2011 DOJ REPORT, *supra* note 80, at 2.

[83] 2009 DOJ REPORT, *supra* note 80, at 1; 2011 DOJ REPORT, *supra* note 80, at 1.

[84] SEN. DIANNE FEINSTEIN AND SEN. SAXBY CHAMBLISS, S. SELECT COMM. ON INTELLIGENCE, 112TH CONG., DEAR COLLEAGUE LETTER (Feb. 8, 2011), *available at* http://big.assets.huffingtonpost.com/SelectCommitteeIntelligenceFeb13.pdf.

[85] 156 Cong. Rec. H838 (daily ed. Feb. 25, 2010) (statement of Rep. Alcee Hastings).

[86] Josh Gerstein, *Official: 13 Briefings for Hill on Call-Tracking Legal Provision*, POLITICO (June 8, 2013), http://www.politico.com/blogs/under-the-radar/2013/06/official-briefings-for-hill-on-calltracking-legal-165732.html.

Congress's reauthorization votes effectively ratified the executive's interpretation of section 215.[87] What matters for our purposes is that the executive went to unusual lengths to inform Congress about the program in an effort to obtain its assent.

In addition to Congress, the FISA court plays a key role in overseeing the NSA programs. Both initiatives involve various forms of ex ante judicial scrutiny. The telephony metadata program is reviewed every three months, when a prior court order authorizing collection expires and comes up for renewal. The court most recently reauthorized the program on June 19, 2014,[88] after having issued an opinion on August 29, 2013 detailing its conclusion that the program is constitutionally and statutorily permissible.[89] Likewise, the FISA court examines the government's section 702 surveillance applications before approving collection of certain international communications for a period of one year.[90] The court is also responsible for reviewing and approving the minimization procedures that govern how both programs operate in practice.[91] Again, the FISA court's role in overseeing programmatic surveillance represents a sharp departure from the historic norm. In the 1980s, when the NSA was engaging in bulk collection of satellite-based international communications (which Congress specially exempted from regulation under FISA), the court played no part in overseeing those operations.

The FISA court is often derided as a rubber stamp. But there are a number of indications that it does in fact serve as a real constraint on the executive branch. Over the three month period between July and September 2013, the court refused to approve nearly a quarter of the government's surveillance requests, insisting on "substantive changes" before okaying the applications—e.g., requiring officials to submit

---

[87] Section 215 Ruling, *supra* note 15, at 23-27; ACLU v. Clapper, No. 13 Civ. 3994, 2013 WL 6819708, at *4 (S.D.N.Y. Dec. 27, 2013); *see also* Benjamin Wittes & Jane Chong, LAWFARE BLOG (Sept. 19, 2013, 12:03 AM), http://www.lawfareblog.com/2013/09/congress-is-still-naked/. *But see* Orin Kerr, THE VOLOKH CONSPIRACY (Sept. 17, 2013, 7:39 PM), http://www.volokh.com/2013/09/17/thoughts-august-2013-fisc-opinion-section-215/ (criticizing FISA court's ratification analysis).

[88] Joint Statement From the ODNI and DOJ on the Declassification of Renewal of Collection Under Section 501 of FISA (June 20, 2014), *available at* http://www.dni.gov/index.php/newsroom/press-releases/198-press-releases-2014/1082-joint-statement-from-the-odni-and-doj-on-the-declassification-of-renewal-of-collection-under-section-501-of-fisa.

[89] Savage, *Extended Ruling*, *supra* note 15.

[90] 50 U.S.C. § 1881a(a) (2012).

[91] 50 U.S.C. § 1861(g) (section 215 program), §1881a(e) (section 702 program).

more information to justify the monitoring or altering the scope of the authority sought.[92] The FISA court may not say "no" very often, but it pretty frequently says "not yet."

Recently declassified documents suggest that the FISA court has meaningfully checked NSA bulk collection in particular.[93] In May 2011, the administration told the FISA court about an over-collection problem in the PRISM program. Because of the way some communications are bundled, the NSA had been collecting some purely domestic communications (which may not be intercepted under section 702) in the course of collecting communications involving persons reasonably believed to be outside the United States (which may). After a series of written submissions, meetings between court and government personnel, and a hearing, the court on October 3, 2011 issued an 81-page opinion concluding that the program violated both the Fourth Amendment and section 702, principally because the NSA's minimization procedures were inadequate.[94] The government responded by developing new procedures to segregate the permissible intercepts from the impermissible ones, applying the procedures to previous acquisitions, and purging tainted records from its database. The FISA court then ruled in opinions dated November 30, 2011 and September 25, 2012 that the revised program passed muster. A 2009 episode involving the telephony metadata program followed a similar pattern—the executive's discovery of violations, disclosure to the FISA court, judicial rebuke, institution of reforms, and judicial approval of the revised program.[95]

At one level this is a dishearteningly familiar story of government misconduct. But the deeper lesson the episode reveals is that, when confronted with such errors, the FISA court is willing to intervene and

---

[92] *See* Letter from Reggie B. Walton, Presiding Judge, FISA Ct., to Charles E. Grassley, Ranking Member, Sen. Comm. on the Judiciary 1 (Oct. 11, 2013), *available at* http://www.lawfareblog.com/wp-content/uploads/2013/10/ranking-member-grassley-letter-131011.pdf.

[93] *See* Ellen Nakashima, *NSA Gathered Thousands of Americans' E-mails Before Court Ordered It to Revise Its Tactics*, WASH. POST (Aug. 21, 2013), http://www.washingtonpost.com/world/national-security/nsa-gathered-thousands-of-americans-e-mails-before-court-struck-down-program/2013/08/21/146ba4b6-0a90-11e3-b87c-476db8ac34cd_story.html.

[94] October 3, 2011 Section 702 Ruling, *supra* note 21, at 2.

[95] Ellen Nakashima et al., *Declassified Court Documents Highlight NSA Violations in Data Collection for Surveillance*, WASH. POST (Sept. 10, 2013), http://www.washingtonpost.com/world/national-security/declassified-court-documents-highlight-nsa-violations/2013/09/10/60b5822c-1a4b-11e3-a628-7e6dde8f889d_story.html.

enforce basic constitutional and statutory guarantees—which is exactly what we would expect an Article III court to do. The PRISM incident also suggests that the government takes seriously its obligations to self-police and disclose problems to the court. Indeed, officials have an interest in doing so. The government's ability to persuade the FISA court to approve its surveillance requests depends in large part on its credibility with the judges. And that goodwill would dissipate if the court independently learned, such as though leaks, about violations that officials had failed to disclose. It would be a mistake to take too much comfort from this incident, since it is impossible to say how representative it is. Still, it provides some reason for optimism that FISA court oversight—and the internal oversight on which it depends—is more than perfunctory.

A third noteworthy feature of PRISM, though not the metadata program, is the unusual transparency surrounding its adoption. PRISM appears to be a straightforward application of FISA section 702, which Congress enacted in 2008. The legislation was the result of a lengthy and detailed public debate touched off by revelations in late 2005 that the Terrorist Surveillance Program was intercepting certain international communications without judicial approval. During the ensuing three year national conversation, intelligence officials repeatedly explained to Congress and the public why they thought new statutory authority was necessary, and advocacy groups and other interested parties repeatedly challenged these representations and urged Congress to reject, or at least curtail, any new surveillance powers. Newspaper editorial pages, blogs, talk radio programs, and many other media organs hashed out the legal and policy issues. FISA was front-page news. In short, the section 702 program shouldn't come as a surprise because the nation thoroughly debated it for three years before Congress expressly approved it.

While the NSA programs feature several important safeguards to help protect privacy and civil liberties, there is room for improvement. Policymakers should consider altering the minimization rules to better prevent mission creep, adding an adversarial element to certain aspects of the FISA court's proceedings, and enacting new legislation to place the telephony metadata program on a more stable statutory footing.

First, the minimization rules that govern the section 702 program allow intelligence officials to share information with federal law enforcement if it contains "evidence [of] a crime."[96] The government

---

[96] Minimization Procedures Used by the National Security Agency in Connection with Acquisitions of Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as Amended at 5 (July 28, 2009), *available at* https://s3.amazonaws.com/s3.documentcloud.org/documents/716634/exhibit-b.pdf.

recently has clarified that "nonpublicly available signals intelligence that the United States collects in bulk" may only be used to counter certain enumerated national security threats, as well as "[t]ransnational criminal threats."[97] Even with that restriction, however, the rules seem too permissive. On their face, the minimization rules permit the fruits of PRISM surveillance to be used in investigations of even minor federal offenses, such as mail fraud and theft, so long as they have some "[t]ransnational" aspect. The problem is that the relative costs and benefits of surveillance depend on the magnitude of the offense under investigation. Just because we're willing to countenance the use of extraordinary methods to prevent terrorism, it doesn't mean the same techniques should be used to combat tax delinquency. Policymakers should tighten the list of crimes for which sharing is allowed. Of course, intelligence officials certainly should be able to tell their law enforcement counterparts when they come across evidence of terrorism, espionage, and other national security threats—the need for cops and spies to share more counterterrorism information is one of the enduring lessons of 9/11.[98] And other serious crimes like those involving risk of death or serious bodily injury, or child exploitation, should be on the list as well.

At the same time, we should not overestimate the NSA's enthusiasm for sharing the intelligence it gathers. Regardless of what the minimization rules permit, the NSA will have strong incentives to resist sharing information with or otherwise helping its bureaucratic rivals.[99] Indeed, the *New York Times* recently reported widespread frustration among law enforcement officials over the NSA's reluctance to assist their investigations of routine offenses like "money laundering, counterfeiting and even copyright infringement"; their requests are usually denied "because the links to terrorism or foreign intelligence" are considered too "tenuous."[100] (Note that the story addresses NSA resources in general, not telephony metadata and PRISM data in particular.) In short, institutional self-interest and

---

[97] OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE, LIST OF PERMISSIBLE USES OF SIGNALS INTELLIGENCE COLLECTED IN BULK (Feb. 10, 2014), http://icontherecord.tumblr.com/post/76245354008/list-of-permissible-uses-of-signals-intelligence.

[98] *See, e.g.*, 9/11 COMMISSION REPORT, *supra* note 68, at 416-19.

[99] *See* Nathan Alexander Sales, *Share and Share Alike: Intelligence Agencies and Information Sharing*, 78 GEO. WASH. L. REV. 279 (2010).

[100] Eric Lichtblau & Michael S. Schmidt, *Other Agencies Clamor for Data N.S.A. Compiles*, N.Y. TIMES (Aug. 3, 2013), http://www.nytimes.com/2013/08/04/us/other-agencies-clamor-for-data-nsa-compiles.html?pagewanted=all.

legal restrictions on sharing can be rough substitutes. And while self-interest will often lead the NSA to refuse access to sensitive intelligence in garden-variety criminal cases, these naturally occurring bureaucratic incentives should be supplemented with strong minimization rules that prevent inappropriate mission creep.

Second, Congress's decision to subject the executive branch's surveillance requests to ex ante judicial review—one of the most important innovations of the original 1978 FISA—has created a powerful tool for preventing overreach. But this mechanism has its limits, because the FISA court's proceedings are conducted ex parte.[101] This can deprive the court of the benefits of the ordinary adversarial process, which relies on the presentation of opposing points of view to sharpen and refine legal and factual disputes. For that reason, policymakers should provide for adversarial review in the FISA court in certain circumstances. Adversarial proceedings would harmonize with the commonplace intelligence technique known as "red teaming," in which special groups of analysts improve intelligence products by preparing assessments that challenge consensus views.[102]

The need to add some sort of adversarial element to FISA has quickly become conventional wisdom, having been embraced by both major NSA reform bills in Congress (Feinstein-Chambliss[103] and Leahy-Sensenbrenner),[104] by the President's Review Group,[105] and by President Obama himself.[106] Indeed, at press time, Congress is poised to enact legislation that generally would require the FISA court to appoint an adversarial "special advocate" in any case that "presents a novel or significant interpretation of the law," though some commentators object that this mandate doesn't go far enough.[107]

---

[101] 50 U.S.C. § 1805(a) (2012).

[102] LOWENTHAL, *supra* note 25, at 146.

[103] FISA Improvements Act, S.1631, 113th Cong. § 4 (2013).

[104] USA FREEDOM Act, S.1599, 113th Cong. § 401 (2013).

[105] PRESIDENT'S REVIEW GROUP, *supra* note 32, at 36, 203-05.

[106] *See* Scott Wilson & Zachary A. Goldfarb, *Obama Announces Proposals to Reform NSA Surveillance*, WASH. POST (Aug. 9, 2013), http://www.washingtonpost.com/politics/obama-to-announce-proposals-to-reform-nsa-surveillance/2013/08/09/ee3d6762-011a-11e3-9711-370831of6f4d_story.html.

[107] *See, e.g.*, Steve Vladeck, *The USA FREEDOM Act and a FISA "Special Advocate"*, LAWFARE BLOG (May 20, 2014, 4:19 PM), http://www.lawfareblog.com/2014/05/the-usa-freedom-act-and-a-fisa-special-advocate/.

This is not to suggest that the process for approving surveillance has been entirely lacking in adversarialism. Adversarial review has been present, it just has taken place in the executive branch rather than the FISA court. Surveillance applications typically undergo multiple layers of internal review before presentation to the court, and that process can be exacting. The unit that manages the review process—the Justice Department's Office of Intelligence—routinely pushes back on operators seeking permission to engage in surveillance.[108] The office might insist that the application include more facts to support the claim that a target is a spy or terrorist. Or it might demand a fuller explanation of the expected national security gains. Or it might require stricter privacy rules governing how collected information is to be used. Again, self-interest explains why.[109] Attorneys from the Office of Intelligence want to maintain their enviable record before the FISA court, and the credibility on which that record depends, so they closely scrutinize the proposals that land on their desks. If they seem unlikely to meet the court's approval, they are sent back for revision or rejected outright. This kind of internal review is not a perfect substitute for a traditional adversarial hearing before a court, but it can achieve some of the same benefits.

Nor is this to suggest that *all* FISA court proceedings should contain an adversarial element. The bulk of the court's work is reviewing individualized applications to monitor specific targets, and the benefits of an adversarial process would be relatively slight in this context. This is familiar terrain for federal judges, who routinely approve individualized wiretaps ex parte in regular criminal investigations.[110] Moreover, cutting-edge legal and policy issues are less likely to arise in the course of adjudicating a request to tap a specific person, as these proceedings usually turn on an essentially factual question—i.e., is there probable cause to believe the target is an agent of a foreign power? Adversarial proceedings would be more helpful where the court is asked to approve broad, overarching surveillance programs like the metadata and PRISM initiatives. These proceedings frequently will involve the balancing of basic values like the need to preserve both national security and privacy and civil liberties. In that respect the proceedings can be quasi-legislative and thus would benefit from the presence of diverse viewpoints.

---

[108] *See, e.g.*, BAKER, *supra* note 69, at 54-55.

[109] Sales, *Self-Restraint*, *supra* note 63 at 285-86.

[110] 18 U.S.C. § 2518(3) (2012).

Finally, officials should reconsider whether section 215 is the appropriate statutory vehicle for the government's exploitation of telephony metadata. It seems a stretch to use the equivalent of a grand jury subpoena to collect billions of call records. Moreover, some observers have questioned whether the program is consistent with the underlying statute.[111] Are electronic records (or databases of electronic records) "tangible things" within the meaning of section 215? Is an entire database deemed "relevant" because it contains a handful of records pertinent to counterterrorism efforts? The NSA may well have good reasons to analyze large troves of telephony metadata, but section 215 seems like an awkward way to do it. Congress should enact new legislation that specifically authorizes the program and describes the limits under which it may operate. In fact, Congress is on the verge of making substantial changes to the metadata program as this article goes to press. The legislation would effectively transform it from a programmatic surveillance initiative that involves bulk collection to a more familiar individualized surveillance tool that only allows the NSA to obtain call records from phone companies if the FISA court concludes that they are associated with a "specific selection term" (such as an individual phone number).[112]

***

Big data is probably here to stay. Programmatic surveillance that aims at identifying previously unknown terrorists and spies has the potential to be an important addition to the national security toolkit. And in an era where private companies like Amazon and Google assemble detailed digital dossiers to predict their customers' buying habits, it is more or less inevitable that counterterrorism officials will want to take advantage of the same sorts of technologies to stop the next 9/11. That's why it's critical to establish a set of baseline rules to govern any system of programmatic surveillance. These first principles can ensure that the government is equipped with a valuable tool for preventing terrorist atrocities while simultaneously preserving our national commitment to civil liberties and privacy.

---

[111] *See, e.g.*, Donohue, *supra* note 5, at 603; Jaffer, *supra* note 4, at 88-90.

[112] *See* Savage, *Surveillance Bill*, *supra* note 13.